

DEPARTMENT OF THE ARMY
HEADQUARTERS, UNITED STATES ARMY MATERIEL COMMAND
5001 EISENHOWER AVENUE, ALEXANDRIA, VA 22333-0001

AMC REGULATION
NO. 25-1

12 May 1998

Information Management

ELECTRONIC MAIL

	Paragraph	Page
SECTION I. GENERAL		
Purpose.....	1	2
Applicability	2	2
Scope	3	2
Explanation of abbreviations and terms.....	4	2
References	5	2
Objectives	6	2
Responsibilities	7	3
SECTION II. INFORMATION SENSITIVITY AND SECURITY POLICY		
Information sensitivity and security	8	5
SECTION III. USER POLICY		
General	9	5
Releasing authority	10	7
Signature authority	11	7
Record copies	12	8
SECTION IV. AUTOMATION/TRAINING POLICY		
Defense Message System (DMS).....	13	8
Electronic mail software	14	9
User training	15	9
APPENDIX A. References		A-1
GLOSSARY		Glossary-1

*This regulation supersedes AMC-R 25-1, 30 October 1986.

SECTION I. GENERAL

1. **Purpose.** This regulation outlines the policies, standards, responsibilities, and procedures for using and managing an electronic mail (E-mail) system to conduct official government business throughout the U.S. Army Materiel Command (AMC).

2. **Applicability.** This regulation applies to Headquarters AMC (HQ AMC) and collocated activities; AMC major subordinate commands (MSC) and their subordinate installations and activities; and all separate installations and activities reporting directly to HQ AMC.

3. **Scope.** Electronic mail is the established standard for the transmission of commandwide organizational communications unless specifically prohibited by regulation or legal statute. The use of E-mail is authorized in lieu of the telephone, U.S. Postal Service (USPS), and other local systems involving the movement of hard copy material.

4. **Explanation of abbreviations and terms.** Abbreviation and special terms cited in this regulation are defined in the glossary.

5. **References.** Related publications are listed in **appendix A**.

6. **Objectives.** a. Provide the capability to enhance employee productivity and command responsiveness.

b. Provide a means to relay detailed information in a timely manner and avoid the different interpretations often associated with verbal conversations.

c. Reduce printing, handling and postage costs, speed up delivery, and ultimately attain a "less paper intensive" environment.

d. Provide procedural guidance and direction for E-mail transmission of organizational and individual communications throughout the command.

e. Establish procedures for the creation, transmission, storage, and disposition of information in electronic format.

7. **Responsibilities.** a. The AMC Deputy Chief of Staff for Corporate Information (DCSCI) will--

(1) Manage AMC's electronic mail program.

(2) Establish plans, policies, regulations, guidelines, and procedures for using the E-mail system.

(3) Assess effectiveness and compliance with E-mail policies, procedures, and standards.

(4) Conduct or require research and studies to be conducted for the development of new or improved approaches to E-mail.

b. Corporate Information Officers (CIO), Deputy Chiefs of Staff for Information Management (DCSIM), and Directors of Information Management (DOIM) will--

(1) Serve as the command source of expertise for electronic mail. Maintain E-mail software. Modify software to run on additional computer systems, as needed. Work with the DCSCI to design and implement an automated information system (AIS) and communications architecture to support a commandwide E-mail system. Include records management requirements when system planning is initiated and during the life cycle of the system.

(2) Conduct research and studies to develop new and improved approaches to E-mail. Develop or otherwise achieve a means to enter an "electronic signature" onto documents passed through the E-mail system.

(3) Develop, maintain, extend, and operate the E-mail program. Monitor the overall efficiency, effectiveness, reliability, dependability, and security of the system and its constituent elements.

(4) Serve as the distributing agent for electronic mail.

(5) Plan, budget, acquire, install, operate, and maintain computer hardware, software, communications, and networks to support the E-mail system.

(6) Appoint a System Administrator to--

(a) Ensure that E-mail software is accredited at the highly sensitive level.

(b) Disseminate procedures and provide user training for using the local E-mail system.

(c) Maintain organizational and individual mailboxes on a local area network (LAN) or wide area network (WAN).

(d) Add mailboxes for newly assigned individuals or established offices. Delete mailboxes upon transfer of individuals or upon reorganization of offices. Create and distribute alias files with the mailboxes of all individuals to all local computers.

(e) Manage the user ID (LOGIN) and password system per AR 380-19.

(f) Monitor files of undelivered mail logs to ensure reliability and timeliness of the local E-mail system. Return all undeliverable mail to the sender or forward to the addressee(s). Notify the sender of the correct address and indicate that the message was delivered to the addressee(s).

(g) Investigate all complaints from users about inappropriate electronic transmissions and determine their validity.

(7) Develop and implement procedures to preserve the record copy of all official E-mail transmissions documenting the official business of the command per AR 25-1, paragraph 8-8, and AR 25-400-2, Chapter 3.

SECTION II. INFORMATION SENSITIVITY AND SECURITY POLICY

8. **Information sensitivity and security.** a. Organizational and individual E-mail messages will be transmitted only over approved and accredited networks. As a minimum, all activities using E-mail software will accredit their system at the "highly sensitive level."

b. The E-mail system may be used to transmit all levels of unclassified sensitive and nonsensitive information. For example, asset, resource accounting, and authorization information, FOR OFFICIAL USE ONLY (FOUO) information, information subject to the Privacy Act of 1974, proprietary and contractual information, and sensitive information including data that may be vulnerable to fraud, theft, misuse, or misrepresentation.

c. Applicable provisions of AR 380-19 will be followed to protect all information processed through the E-mail system. A "need-to-know" will be established and transmitted information will be limited only to that required. Access to workstations and the E-mail system will be restricted to authorized individuals. Utmost care will be taken to protect electronic message files from unauthorized access. Users will comply with the provisions governing FOUO information and information subject to the Privacy Act of 1974.

SECTION III. USER POLICY

9. **General.** a. An authorized user of an AMC E-mail system is any individual possessing the necessary hardware/software and a requirement to send and receive E-mail.

b. Electronic mail will be used where the benefits of cost, timeliness, or productivity can be realized. Users are encouraged to transmit official correspondence via E-mail rather than through official mail and distribution channels.

c. Electronic mail will be used to transmit and receive messages, information summaries, documents, numbered forms, and correspondence such as memoranda, information papers, and information in any form accommodated by the E-mail system.

d. The E-mail system will include specific information in the FROM field. As a minimum, the sender's name (as in the signature of correspondence) will be included in messages from an individual mailbox and the complete name and office symbol of the sending office will be included in messages from an organizational mailbox.

e. Suspense actions received via the E-mail system from outside the chain of command will be brought to the attention of management. It is important to inform management of all suspense actions received from external sources.

f. Users of the E-mail system will--

(1) Ensure that classified information is not entered, stored, or transmitted through the unclassified E-mail system.

(2) Ensure that information is protected per AR 380-19 and AR 380-380.

(3) Provide information to the System Administrator who will maintain an accurate and current list of LOGIN names and mailboxes.

(4) Monitor mailboxes and respond to/act upon incoming messages as required. Ensure that the individual/organization is the appropriate recipient or notify the originator as soon as possible.

(5) Abstain from sending messages that could reasonably be expected to cause excessive strain, directly or indirectly, on any computing facilities or the unwarranted or unsolicited interference with the use of E-mail or an E-mail system by other individuals.

(6) Submit all complaints concerning inappropriate electronic transmissions to the system administrator of an E-mail system.

(7) Be conscientious in the use of an E-mail system to avoid overburdening communications systems and avoid making it

necessary to use scarce Army resources to eliminate service disruptions that could be easily avoided.

10. **Releasing authority.** a. The releasing authority for organizational E-mail transmissions is responsible for final administrative review/approval and will ensure that--

(1) The information conforms with the policies of the Commander or head of the organization and that it has been fully staffed/coordinated.

(2) The author has complied with the provisions of this regulation and other related directives.

b. An individual is the releasing authority for his/her mailbox. No individual may release E-mail from another individual's mailbox. The system administrator is authorized to release (delete) mail files when an individual departs the organization.

c. Individual(s) having password access to an organizational mailbox constitute the releasing authority for E-mail transmitted from that mailbox. The Commander or head of an organization may further constrain the releasing authority as necessary.

d. AR 380-19 prohibits the sharing of passwords between individuals.

11. **Signature authority.** a. Organizational E-mail documents the official business of the command and/or expresses the will of the Commander. The signature authority for release of organizational E-mail may be delegated in writing to subordinates per AR 25-50, Preparing and Managing Correspondence.

b. Documents requiring signature authority may be sent via E-mail. Official correspondence and E-mail documents will be dated and the signature block will be considered unsigned unless signature is indicated. For systems unable to record, transmit, and display electronic or password-generated signatures, the signature block will be transmitted with the words "signed" or "signed by for."

12. **Record copies.** a. The record copy of all official correspondence transmitted or received via the E-mail system will be maintained by the office with access to the organizational mailbox.

b. Electronic records will be identified, maintained, and disposed of per AR 25-400-2, Chapter 3, and General Records Schedule 20 issued by the National Archives and Records Administration. The record copy will reflect all coordination obtained.

SECTION IV. AUTOMATION/TRAINING POLICY

13. **Defense Message System (DMS).** a. The DMS will replace the resource intensive and antiquated automated digital network (AUTODIN), telecommunication centers (TCC), and the existing legacy electronic mail (E-mail) systems currently in use throughout the Department of Defense (DOD). The AUTODIN is scheduled to close in December 1999.

b. The DMS will provide writer-to-reader electronic messaging service access to and from worldwide DOD locations, including tactical deployed users, other designated Federal government users, and interface to allied users and defense contractors. It provides a single capability to the end user (writer/reader) for organizational (official) and individual (informal) messaging service while at home base, traveling, or tactically deployed. Users will transmit and receive messages from their desktop workstations. User authentication and security will be provided by a FORTEZZA card.

c. The DMS consists of all hardware, software, procedures, standards, and facilities used to exchange messages electronically between organizations and between individuals within the DOD and among other authorized users.

d. The current subsystems of the DMS are AUTODIN and E-mail, both host and local area networks (LAN) based, including messaging and mail capabilities implemented for the strategic, sustaining base, and tactical environments.

e. For guidance on incorporating DOD tenant activities at AMC installations into the DMS, refer to HQ AMC memorandum,

5 May 97, subject: AMC Policy on Implementation of Tenant Activities at AMC Installations into the Defense Message System (DMS).

14. Electronic mail software. a. Many available E-mail software packages will run on different hardware and support various configurations. AMC recommends using Microsoft Exchange and Lotus Notes user agents. The preferred is Microsoft Exchange. The software package must be DMS-compliant.

b. Acquisition of commercial E-mail software that will allow users to communicate only with others using the same software is prohibited. Commercial software will be acquired only if it allows its users to communicate with remote users and is DMS-compliant.

15. User training. Every user of an AMC E-mail system will receive guidance on--

a. How to distinguish Federal records from nonrecord materials and personal documentary materials.

b. How to determine when drafts and working papers are Federal records.

c. How and when to generate a recordkeeping copy of an E-mail message.

d. How to mark or classify documents for filing or incorporation into an electronic or hard copy (paper-based) recordkeeping system.

e. How to contact the installation/activity records manager or coordinator for assistance.

Commanders and supervisors at all levels will ensure that users of an E-mail system are cognizant of permissible and unauthorized uses of the system. Users must know that the inappropriate use of an AMC E-mail system may be the basis for consideration of disciplinary action against soldiers and civilian employees.

The proponent of this regulation is the United States Army Materiel Command. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Commander, HQ AMC, ATTN: AMCIO-F, 5001 Eisenhower Avenue, Alexandria, VA 22333-0001.

FOR THE COMMANDER:

OFFICIAL:

JAMES M. LINK
Major General, USA
Chief of Staff

LEROY TILLERY
Chief, Printing and Publications
Branch

DISTRIBUTION:

Initial Distr H (44) 1 ea HQ Acty/Staff Ofc
LEAD (SIOLE-DO-I) (2)
AMCIO-I-SP stockroom (15)
AMCIO-F (2)
Separate Reporting Activities (SRA) (2 ea)
AMCOM/AMSAM-RM-FD (4)
AMCOM/AMSAM-SMO (Library) (4)
ARL/AMSRL-CI-TG (4)
CBDCOM/AMSCB-CIR (4)
CECOM/AMSEL-IM-BM-I (4)
IOC/AMSIO-IML (4)
LOGSA/AMXLS-IM (4)
SSCOM/AMSSC-S-IMS (4)
STRICOM/AMSTI-CS (4)
TACOM/AMSTA-DRM (4)
TECOM/AMSTE-CT-N (4)
USASAC/AMSAC-IM-O (4)

APPENDIX A

REFERENCES

RELATED PUBLICATIONS

AR 18-7	Automatic Data Processing Management
AR 25-1	The Army Information Resource Management Program
AR 25-11	Record Communications and the Privacy Communications System, Chapter 13
AR 25-50	Preparing and Managing Correspondence
AR 25-400-2	The Modern Army Recordkeeping System (MARKS), Chapter 3
AR 340-21	The Army Privacy Act Program
AR 380-19	Information Systems Security
AR 380-380	Automation Security

GLOSSARY

Section 1. ABBREVIATIONS

AIS	Automated Information System
AMC	U.S. Army Materiel Command
AUTODIN	Automated Digital Network
CIO	Corporate Information Officer
DCSCI	Deputy Chief of Staff for Corporate Information
DCSIM	Deputy Chief of Staff for Information Management
DMS	Defense Message System
DOD	Department of Defense
DOIM	Director of Information Management
FOUO	For Official Use Only
HQ	Headquarters
LAN	local area network
MSC	major subordinate command
TCC	Telecommunication Center
USPS	U.S. Postal Service
WAN	wide area network

Section II. TERMS

DISN

Defense Information Systems Network. A computer-based packet switching network utilized within the DOD for long-haul communications.

E-MAIL

A computer-based electronic mail system used to send and/or receive information over local/wide area networks.

LOGIN

A synonym for a user ID. Enables the system to identify users of the system.

MAILBOX

A computer file or equivalent network accessible delivery point which can be located by computer network delivery processes. In many ways, mailboxes are analogous to U.S. Postal Service (USPS) mailboxes. Only the network delivery service can move mail from one mailbox to another.

PASSWORD

A protected word or string of characters to identify or authenticate a user, specific resource, or access type per AR 380-19, Information Systems Security, and AR 380-380, Automation Security). When passwords are entered through the keyboard, the characters are not displayed on the screen. This prevents other people from discovering the password and using it to gain access to the system.